A Review of Distributed Access Control for Blockchain Systems towards Securing the Internet of Things

Citation for the original published paper (version of record):
Butun, I., Österberg, P. (2021). A Review of Distributed Access Control for Blockchain Systems towards Securing the Internet of
Things. IEEE Access, 9: 5428-5441. http://dx.doi.org/10.1109/ACCESS.2020.3047902

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 21, 2020, accepted December 7, 2020, date of publication December 29, 2020,
date of current version January 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3047902

A Review of Distributed Access Control for Blockchain Systems Towards Securing the Internet of Things

ISMAIL BUTUN[1,2], (Member, IEEE), AND PATRIK ÖSTERBERG[3], (Member, IEEE)
[1]Department of Computer Engineering, Chalmers University of Technology, SE-412 96 Göteborg, Sweden
[2]Department of Computer Engineering, Konya Food and Agriculture University, 42080 Konya, Turkey
[3]Department of Information Systems and Technology, Mid Sweden University, 851 70 Sundsvall, Sweden

Corresponding author: Ismail Butun (ibutun@mail.usf.edu)

This work was supported by the Swedish Knowledge Foundation (KKS) under grant research profile Nästa generations Industriella IoT (NIIT).

ABSTRACT As the Internet of Things (IoT) paradigm gets more attention from academia and industry, implementation tools of IoT will be explored more and more. One example is the applicability of blockchain systems to provide security and privacy of IoT networks, which is the topic of this article. Blockchain systems are on the rise, as crypto-currency payment systems (such as Bitcoin, Litecoin, etc.) boomed in the last few years due to their attractive de-centralized and anonymous features. As in every transaction, access of the users to IoT systems needs to be controlled. However, these systems are peer-to-peer systems and do not have centralized control, which means that traditional access control techniques will not be optimal. As a result, distributed access control schemes are needed and this paper aims at providing the state of the art in the literature. Thereby, we introduce and discuss the details and applicability of centralized (role-based) and distributed (threshold-signature, reputation, trusted-computing, identity, capability, ACL, group-signature, and hybrid) access control schemes to blockchain systems under the IoT ecosystems. Moreover, permissioned vs. permissionless blockchain systems are also discussed. Finally, challenges and research directions related to the application of all those presented blockchain systems to IoT are discussed.

INDEX TERMS IoT, survey, P2P, security, Bitcoin, permissioned, permissionless, ledger, LoRa.

I. INTRODUCTION

Internet of Things (IoT) is having its boom era now, as the Internet had two decades ago. Accordingly, the IoT market is growing and expected to reach to a number of 75 billion by 2025 [1], and 500 billion by 2030 [2].

With the proliferation of IoT enabling technologies such as LoRa (**Lo**ng-**Ra**nge), application domains of IoT are expected to grow in various fields including following areas but not limited to [3]–[5]:

- **Smart Electric, Gas and Water metering:** This field is expected to witness the biggest growth rate. Traditional power grid is being replaced by its smarter counterpart, i.e. smart-grid, and therefore smart-metering is one of the most important component that lets us understand the energy consumption at all the levels of the power grid. The adoption of IoT technology by this sector would promote rapid standardization among various smart-meter manufacturers and vendors.
- **Oil and gas operations:** IoT connected devices and systems can provide more efficient oil and gas operations, by requiring minimum human-intervention, and constitute higher value than legacy technologies.
- **Smart cities:** According to [6], LoRaWAN (LoRa-based Wide Area Network) has been selected as an enabling technology to monitor not only light illumination levels (monitoring of street lighting), but also traffic intensity and air pollution levels of a smart city application.
- **Healthcare:** Activity of Daily Living (ADL) helps to indicate health status and capabilities of the individuals in terms of heath care and quality living. In the recent past, most common ways to capture ADL data includes costly day long observations by assigned health-care personnel, self-reporting by the users themselves with great efforts, or in the most primitive way, filling out

The associate editor coordinating the review of this manuscript and approving it for publication was Antonino Orsino.

a written ADL survey. However, proliferation of IoT sensing technologies pave the path towards automated ADL reading, as deeply discussed in [7].

- **Livestock monitoring:** In another project called *Cattle Traxx*, LoRaWAN has been used for remote-monitoring of the cows in a farm by using electronic-tracking ear tags [8].

This work is an extremely enhanced version of the previous work, which presented the access control for wireless sensor networks [9]. Now the paper discusses applicability of the distributed access control over blockchain systems within the scope of IoT security. The paper aims at two important goals: 1) Providing the state-of-art on access control systems proposed for Peer-to-Peer (P2P) networks and elaborate on their applicability to permissioned-BCSs, 2) Discuss and predict applicability of permissioned-BCSs to IoT networks, especially for increasing security in the IoT networks.

There are many perspectives exist in the literature for the presentation of Blockchain: Consensus type (public, private, and consortium), consensus algorithm (Proof-of-Work, Round Robin, Byzantine-Fault Tolerance, Proof-of-Stake, etc.), access control (permissioned vs. permissionless), network structure (centralized vs distributed), etc. [10]. Moreover, recently presented Blockchain algorithms for IoT in the literature can be categorized into 3 major groups based on the 'role' of the blockchain [11]: 53% on *Data Storage*, 28% on *Access Control Mechanism*, and finally 19% on *Platform connector and incentive distributor*. In this article we pick the access control presentation of Blockchain and seek for its' application as an access control mechanism for IoT.

Owing to the absence of a physical line-of-defense, cyber-security of IoT is of a big concern to the scientific community [12]. In this work, it is argued that Blockchain Systems (BCSs) can be leveraged by IoT networks (for instance LoRa-based IoT networks) to increase security. However, traditional permissionless-BCSs such as electronic cash systems (Bitcoin, Litecoin, etc.) cannot be used in special applications presented above due to the long transaction times. At this point, permissioned-BCSs would help. Permissioned-BCSs require access control to improve the security of the overall system and to decrease the transaction time in the blockchain.

The main focus of this manuscript is justifying the applicability of P2P access control schemes for the security of IoT-based Block Chain Systems. As such, the organization for the rest of the work is as follows: Section II provided background on P2P networks (Section II-A) and on access control (Section II-B). Section II-C provides a small introduction to BCSs. Section III presents a thorough literature review of access control systems proposed for P2P networks, whereas Section IV discusses on the selection of those schemes to be employed by the permissioned-BCSs. Section V elaborates on the applicability of permissioned-BCSs to LoRa-based IoT networks. Finally, Section VII concludes the paper and draws the future work.

II. BACKGROUND

Blockchain is a relatively new technology proposed for digital crypto-currencies. This idea was originally designed and invented by Bayer *et al.* [13] in 1992 and included Merkle trees to provide the efficiency and reliability of the digital time-stamps. Hayek published his classic book of 'Denationalization of Money' [14] in 1976 and argued that money is the same as other commodities and it needs to be supplied by competition among private providers, not by the government. The 'crypto-currency' term has urged from that perspective and nowadays uses the blockchain technology as the back-haul system for the transactions [15]. Besides, crypto-currency also attracted public attention to the blockchain technology, allowing researchers and developers to work and innovate by transforming and providing this technology for today's challenging needs.

Blockchain-based security algorithms provide decentralized solutions but involve significant energy, delay and computational overhead which is not suitable for resource constrained devices of the IoT. For example, Dorri *et al.* [16] have proposed usage of blockchain technology in security and privacy of IoT. In the proposal, high processing enabled miner devices are employed and additionally attached to the home network, to provide needs and functionalities of the blockchain algorithms. However, proof-of-concept applications need to be developed and further analyzed in this manner.

Hence the aim of this manuscript does not include detailed representation of blockchain systems, the readers are suggested to read following references for that purpose: [11], [17]–[21]. Moreover, interested readers are recommended to follow; [22]–[24] for the cyber-security of Blockchain systems, and [25]–[28] for background on the cyber-security of IoT networks.

As blockchain network being a type of Peer-to-Peer (P2P) networks, in the rest of this section, P2P networks are first introduced, then access control schemes proposed for P2P networks are investigated. Then, a brief introduction and classification of blockchain systems (BCSs) is introduced. Finally, BCSs and their applicability to IoT Networks is thoroughly elaborated for various application domains.

A. PEER-TO-PEER (P2P) NETWORKS

A P2P network is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or stable hosts). Peers are both suppliers and consumers of resources, in contrast to the traditional client–server model where only servers supply, and clients consume. A P2P network architecture is shown in Fig. 1 which consists of peers and lacking dedicated infrastructure such as servers and back-end devices [29].

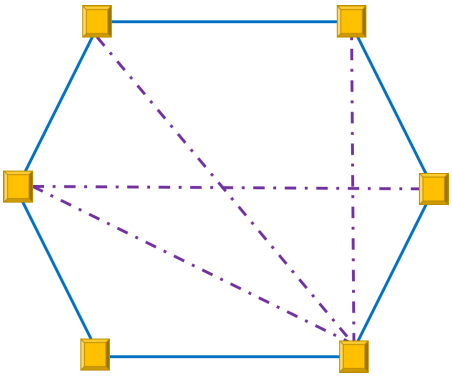

FIGURE 1. Representation of the architecture of a Peer-to-Peer (P2P) network consisting 6-nodes.

There are 3 classes of P2P applications that is worth to mention:

- **Parallelizable:** Splits a large task into smaller pieces that execute in parallel at a number of independent peer nodes
- **Content-based:** Focuses on storing information at various peers in the network. Operates in a disconnected, asynchronous manner.
- **Collaborative:** Allows peers to collaborate in real time, without relying on central servers to collect and relay information. Upcoming collaborative P2P networks are looking for diverse peers that can bring in unique resources and capabilities to a virtual environment thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers [30].

There are several unique characteristics of P2P networks which bring their own challenges along with: First of all, there is an absence of server infrastructure and also lack of trusted authority. Secondly, there is a dynamic type of membership which often implies dynamic topology that complicates routing as well as security. Besides, it demands for opportunistic collaboration, meaning that collaborated members are rewarded. Finally, the content management such as placement and retrieval is also another non-trivial task to be fulfilled.

Here is an overview of vast application areas of P2P networks:

- **Content Delivery:** In P2P networks, clients both provide and use resources. This means that contrary to client-server systems, the content-serving capacity of P2P networks can actually increase as more users start to access the content. This property is one of the major advantages of using P2P networks because it makes the setup and operation costs very small for the original content distributor. [29] These are mostly known to be file sharing platforms: Gnutella, Kazaa, Napster, EMule, eDonkey, Lime, etc.
- **Finance:** Blockchain payment systems (electronic cash systems) such as Bitcoin, Ethereum, Litecoin, etc.
- **Networking:** Dalesa (a P2P web cache for LANs) is a free and opensource software developed by Lanka Software Foundation under GPL license. Dalesa can be used as an alternative to centralized web caches in a LANs. This is done by exposing the cashes of the local web browser to the whole P2P network [31].
- **Science:** In bio-informatics, drug identification search engines, scientific file sharing (Sci-Hub).
- **Voice over IP (VoIP):** Voice over Internet Protocol (VoIP), also known as IP telephony, is a method of technologies for the delivery of voice communications and multimedia sessions over IP networks, such as the Internet. Discord, Skype, Google Talk, etc. are examples of commonly known VoIP applications. VoIP is achieved by special protocols, such as Jingle, which is an extension to the Extensible Messaging and Presence Protocol (XMPP) that adds up P2P signaling for VoIP communications [32].
- **Defense:** Modern warfare network projects by DARPA (USA) take advantage of this technology. For instance, small cameras use P2P networking technology to fuse data into high-resolution color images in PIXNET project. While PIXNET works on inter-squad P2P image sharing, other DARPA programs are focused on using soldiers' smartphones as servers in inter-squad-level networks [33].

B. ACCESS CONTROL

The term *Access Control* refers to the control over system resources after a user's account credentials along with the identity have been authenticated. As a result of a successful attempt, access to the system or resources is granted. Access can be granted for individual users or for a group of users and granted destination can be a unique or multiple types of resources. For example, a particular user, or group of users, might only be permitted access to some certain files after logging into a system, while simultaneously being denied access to all other resources.

Access Control provides a solution to the *confidentiality* and it is the key mechanism to achieve restricting access to the data sources we want to protect [9], [34]. Access control policies and mechanisms are necessary to ensure that peers only use the resources in an authorized way. Trust is the expectation that a peer will behave in a particular manner for a specific purpose. An access control mechanism must prevent unauthorized peers from becoming a part of the network and to establish trust among members in the absence of a trusted authority.

P2P systems as well as mobile ad hoc groups are categorized as ad hoc groups. These groups are characterized by two key features, the lack of trusted authority, and a dynamic membership which often implies a dynamic topology. These features introduce new challenges such as content placement and retrieval, routing, and security.

Content based P2P application focuses on storing information at various peers in the network and operate in a disconnected, asynchronous manner whilst other applications such as conferencing require synchronous operation.

Access control requirements for P2P Networks are categorized under 2 groups:

1) MAIN REQUIREMENTS OF ACCESS CONTROL FOR P2P NETWORKS

The main requirements that an access control framework for P2P networks should support are:

- **No centralized control or support:** A peer has significant level of autonomy and is in charge of storing and managing its own access control policies (decentralization).
- **Peer classification:** A P2P access control model must provide a mechanism for a host peer to classify users and assign each user different access rights, even if the users were previously unknown.
- **Encourage sharing files:** peers must be confident that participation in the system will give them better chance to access to the files they want.
- **Limit spreading of malicious and harmful content:** A P2P access control system should provide mechanisms to limit such malicious spreading and punish those who are involved in.

2) AUXILIARY REQUIREMENTS OF ACCESS CONTROL FOR P2P NETWORKS

The auxiliary requirements that an Access Control Framework for P2P Networks should support are:

- **Dynamic topology:** Hence Access Control Lists (ACLs) enumerate all possible members permanently, static ACLs cannot be used because of the dynamic topology of the network where memberships change frequently.
- **Autonomy:** Host peer is a standalone system where shared files are objects that need to be protected and client peers are subjects who are considered to possess access rights.
- **Trusted peer authentication and authorization in client platform:** In distributed and decentralized systems, an object or policy owner needs to trust that the valid peer is authenticated and authorized in a client platform before being allowed to access a protected object.

C. BLOCKCHAIN SYSTEMS (BCS)

There are two types of BCSs, public and private [35]:

1) *Public BCSs* are also called 'permissionless' blockchain. The access control is not mandatory for these systems as of now. Bad mannered participants can join the network for ledger operations yet this will not affect overall system, on the assumption that the number of adversaries cannot be more than 50% of the overall network members.
2) *Private BCSs* are also called 'permissioned', 'consortium', or 'hybrid' blockchain. It is used for the systems in which access control is inevitably necessary. Hence, they cater for the ledger needs of private corporations or consortium's.

Please refer to Fig. 2 for the various applications (mostly digital crypto-currencies) fields of permissioned- vs. permissionless-BCSs [36]. Among permissioned-BCS, Tillit and Ripple Labs are based on XRP (Ripple coin), Hyperledger is based on PBFT (Practical Byzantine Fault Tolerance), CryptoCorp and Tembusu are based on BTC (Bitcoin), Eris and Clearmatics are based on Ethereum, and finally, Tezos is based on the consensus-agnostic algorithm.

D. APPLICATIONS OF BCSs TO IoT NETWORKS

In the recent literature, several approaches are proposed as an application of BCSs to IoT (some of which are presented in Kim and Deka's book) [37]. Here, we will classify and present these under 2 major categories:

1) CLASSIFICATION DUE TO THE PROVIDED SECURITY SERVICES

- **Access Control:**
  - Nakamura *et al.* [38] proposes a Capability-Based Access Control (CapBAC) scheme by applying the emerging Ethereum blockchain technology, to provide more fine-grained access control and more flexible token management.
  - Chattaraj *et al.* proposes a Blockchain-based access control scheme for the Software Defined Network SDN) framework [39]. The proposed scheme has the capability to resist various well-known attacks and alleviate the existing single point of controller failure issue in SDN.
  - Riabi *et al.* [40], surveyed BCS-based access control schemes proposed for IoT networks. According to authors, there are two main categories: 1) Transaction-based access control, 2) Smart-contract -based access control. In both of the categories, the aim is to provide an *access token* to the intended user or thing of the IoT. Authors stressed that one of the main benefit of using BCSs as an access control mechanism is to avoid single point of failure, which is the main problem for traditional centralized systems. Riabi *et al.* also proposed their own access control scheme in [41], which relies on BCS to avoid single point of failures (central entity) in IoT. The proposed scheme is a hybrid scheme leveraging ACL, capability-based and identity-based access control schemes.
- **Consent Management:** In [42], Rantos *et al.* proposed a framework that facilitates European General Data Protection Regulation (GDPR)-compliant processing of personal data in IoT networks. Their proposal utilize BCS to support the integrity, the non-repudiation and the

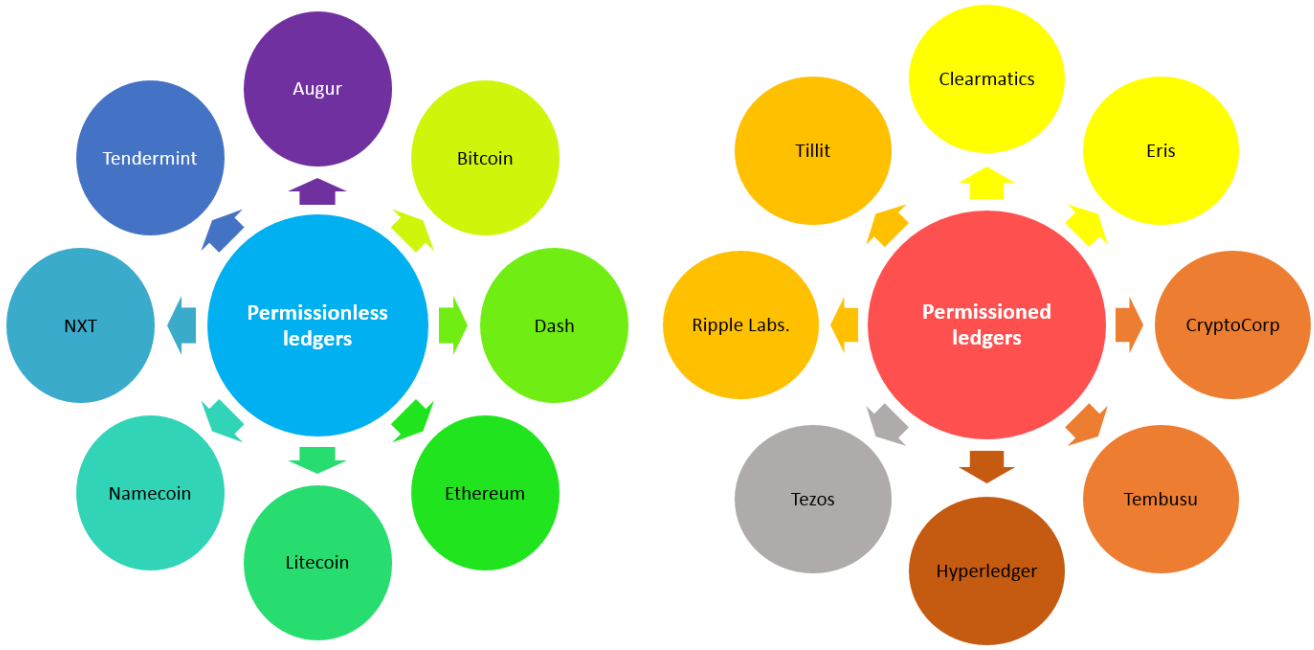

FIGURE 2. Various applications of permissionless vs. permissioned blockchain ledgers.

versioning of consents in a public verifiable way without any trusted party.

- **Hardware-Assisted Security:** In [43], Mohanty *et al.* presented usage of blockchain for sustainable simultaneous device and data security in the IoT, which was particularly focused on the integration of BCSs with hardware security primitives called physical unclonable functions (PUFs) to solve scalability, latency, and energy requirement challenges of the IoT.
- **Intellectual Property Protection:** In [44], Lin *et al.* proposed a system architecture of blockchain and IoT based intellectual property protection system, which can process three types of intellectual property: 1) Patents, Copyrights, Trademarks etc.; 2) Industrial design, Trade dress, Craft works, Trade secrets etc.; and 3) Plant variety rights, Geographical indications etc.
- **Secure Communications:** In [45], Wazid *et al.* presented usage of blockchain for communications security in intelligent IoT, which was particularly focused on the authentication and key management issues. Another secure communication framework is presented in Wazid *et al.*'s work [46], for the Blockchain-Based Intelligent Battlefield IoT environment.
- **Security framework for SDN:** A blockchain enabled distributed security framework for next generation IoT networks by using edge-cloud and software defined networking (SDN) is presented in Medhane *et al.*'s work [47]. Accordingly, the security attack detection is achieved at the cloud layer, and security attacks are consequently reduced at the edge layer of the IoT network.
- **Smart contracts:** Smart contracts can be established for IoT by using Blockchain technology [10].
- **Trust Management:** In [48], Kandah *et al.* present a multi-tier scheme consisting of an authentication- and trust-building/distribution framework designed with blockchain technology to ensure the safety and validity of the information exchanged in the Smart City systems and Connected Vehicle Setups. The blockchain-based trust management scheme aims at creating a trustworthy environment for connected autonomous vehicles. The presented quantitative simulation results point the trade-offs of secure block generation for local and global trust calculations vs. mobility. In [49], Lu *et al.* proposed a trust-management scheme (set-up and distribution) for smart cities and connected vehicles to ensure the safety and validity of the information exchanged in the IoT network based on blockchain technology.

2) CLASSIFICATION DUE TO THE APPLICATION LANDSCAPE

- **Cyber-Physical Systems:** As discussed in Zhao *et al.*'s work [50], Blockchain can play a critical at cyber-physical systems (CPS) where Internet of Things (IoT) are heavily used to collect sensed data regarding the environment and the system being monitored. Moreover, blockchain could encourage and facilitate data and service sharing across multiple organizations because it enforces a standard way of communication and data storage (i.e., interoperability), and has a built-in real-time micro-payment capability.
- **Intelligent Transportation System (ITS):** Vangala *et al.* [51] proposed a new Blockchain-enabled certificate-based authentication scheme for vehicle accident detection and notification in environment, so that

a vehicle can report securely the transactions related to accident detection and notification of its own or neighboring vehicles to its cluster head, Road Side Unit, or edge servers.
- **Smart City:** Dewan and Singh [20] proposed Blockchain-based solution for smart property which provides security against forgery when compared to the traditional centralized database systems. They offered this as a use-case of Blockchain in designing smart city.
- **Supply chain management:** Blockchain can be utilized by supply chain management to track and trace the origin of the food products in agriculture [52].
- **Underwater Things:** In [53], Uddin *et al.* proposes a layer-based architecture consisting of Fog and Cloud elements to process and store the Internet of Underwater Things (IoUT) data securely with customized Lightweight Blockchain technology.

Due to Makridakis and Christodoulou [54], Blockchain's ability towards security and immutability can also be used for storing the highly sensitive, personal data needed to determine patterns in sensitive cases such as those involving the healthcare sector. The future of blockchain might move in two far directions: The first will include all those applications requiring decentralized, super secured networks. IoT, autonomous vehicles, Decentralized Autonomous Organizations, smart contracts would be included in this category. The other direction will include advances in the Artificial Intelligence that when combined with Blockchain can substantially improve its over-all value and application landscape.

As presented above, although there has been new proposals in the field to apply BCSs for the access control of IoT, all of the proposals are in the primitive phase and yet to be proven by implementations, cross comparisons and thorough evaluations. Besides, in most of these proposals, access control is offered through permission-less BCSs which require demanding power and processor consumption, therefore mostly not applicable to the tiny micro devices of the IoT that are used nowadays. More importantly, another critical issue is the total time required for each access process event (login attempt); it would be really bad from Quality of Service point of view (timeliness), if a user is expected to wait several seconds to be granted for the services that he/she would like to use. Especially for the networks and services that require fast response time (real time or close to real time), BCSs have not been used or proven to provide safe operation. Therefore, in this article, ways of improving the access process time is sought, by leveraging especially the schemes designed for distributed P2P networks, as described below.

III. ACCESS CONTROL IN P2P NETWORKS

In the literature, two groups of solutions are proposed for access control problem in P2P networks, based on the location of the decision-taking:

- **Centralized Approach:** A central server stores and evaluates access control policies. A centralized authority identifies users, defines roles and groups, controls the access rights. Central or trusted third parties monitor and manage access control. There is only one type of centralized approach: Role-based.
- **Distributed Approach:** Peers have a significant level of autonomy and are in charge of storing and managing their own access control policies. This can be also considered as distribution of trust from central authority to peers, which is the basic idea behind the execution of recent crypto-currency schemes (a.k.a. blockchain transaction). The proposed solutions for distributed access control in P2P networks are as follows: Threshold signature based, Reputation-based (trust vectors), Trusted computing (platform) based, Identity based, Capability based, ACL based, Group Signature based, and finally Hybrid based; Approach-1 (credential + identity + role), Approach-2 (threshold cryptography + secret sharing + hierarchical identity).

All centralized and distributed access control approaches in the literature are discussed in details as follows:

A. CENTRALIZED ACCESS CONTROL FOR P2P NETWORKS

The only type of centralized access control solution for P2P networks is Role-Based Access Control (RBAC). In RBAC-based approach, the permissions are associated with the roles, and the users are assigned to appropriate roles, thereby acquiring the role's associated permission. Since roles are considered for access control decisions instead of identities, the scalability will be increased in a large distributed P2P environment. Three primary rules are defined for RBAC [55]:

1) **Assignment of the roles:** A subject can execute a transaction only if the subject has been selected or assigned to a role.
2) **Authorization of the roles:** A subject's active role must be authorized for that specific subject. Associated with the rule-1, this rule guarantees that the users can take-on only roles for which they are authorized to.
3) **Authorization of the transactions:** A subject can execute a transaction, only if the transaction is authorized for the subject's current active role. Associated with rule-1 and rule-2, rule-3 guarantees that the users can only execute transactions for which they are authorized to.

In [56], Park *et al.* propose a two-tier ultra-peer architecture in which the access control decisions, searching for resources and resource management are handled by ultra-peers. In this paper, authors introduce an approach for securing transactions in the P2P environment and investigate ways to incorporate RBAC into current P2P computing environments. A regular peer requests a particular resource and the requesting peer's ultra-peer does the query for the resource on behalf of the regular peer. If there is a peer that has the requested source, the providing peer's ultra-peer makes

an access control decision to determine if the requester has the enough privileges. Ultra-peers act as proxies for their leaf-nodes and can provide more effective and scalable access control in dynamic computing environments.

In another proposed scheme of Park and Hwang [57], a manager application, located in the middle-ware of each peer, facilitates provisioning capacities for use of resources and controls usage of resource on behalf of that peer. An integrated model which supports autonomous decisions and centralized controls is introduced. The RBAC model is extended to support access control in a controlled P2P environment. The environment contains a manager who facilitates provisioning capacities for use of resources and controls usage of resource on behalf of a peer. The community and enterprise *User Role Assignments* are maintained in a centralized manner, while the Permission Role Assignments are maintained in a distributed manner. The proposed approach enables a peer to make the access control decision autonomously based on the enterprise, the community and the peer policies without needing other components.

B. THRESHOLD SIGNATURE BASED DISTRIBUTED ACCESS CONTROL

Threshold cryptography (or threshold signatures) is the basic tool to implement distributed access control mechanisms.The idea of threshold signatures applies directly to build access control mechanisms by making collaborative decisions. A prospective member and a set of existing group members interacts in order to approve the new membership. The number of current members taking part in the admission is at least the number necessary for the admission threshold which is less than the total number of group members. $(t + 1, n)$ threshold cryptography employs the secret sharing of the group secret among n members in such a manner that any set of $(t + 1)$ members can recover the group secret and perform a cryptographic operation jointly.

Static ACL cannot be used because of the dynamic topology of the network where memberships change frequently, because ACLs enumerate all possible members permanently. Admission decisions made by a trusted third party (TTP) or a group founder violates the peer nature of the underlying ad hoc group. Decentralized access control is the fundamental security service for ad hoc groups. It prevents unauthorized nodes from becoming members and bootstrapping other security services such as key distribution.

Threshold signature scheme enables any subgroup of t members in a group to collaboratively sign a message on behalf of that group. This is achieved by secret-sharing the signature key among the group members, and allowing them to compute a signature on some message via a distributed protocol in which the members use the shares of the signature key instead of the key itself. Threshold signature schemes can tolerate up to t corruptions in the whole lifetime of the system. The idea of threshold signatures applies directly to build access control mechanisms by making collaborative decisions.

In [58], Saxena *et al.* propose and evaluate four different P2P access control schemes based on various cryptographic techniques:

1) RSA (Rivest-Shamir-Adleman algorithm)-based threshold signature
2) DSA (Digital Signature Algorithm)-based threshold signature
3) Plain signature (PS)
4) Accountable Subgroup Multi-signature (ASM)

Their evaluation results are provided as follows: PS offers lower join cost but longer Group Membership Certificates (GMCs), whereas other schemes, have shorter (ASM) or constant (TS-RSA/TS-DSA) GMCs but high join cost. In these schemes, authentication of the P2P users is the main goal, not their authorization.

In another work of Saxena *et al.* [59], authors propose 3 types of threshold cryptography based access control schemes: DSA-based, BLS-based, and Schnorr-based. Among these, the Schnorr threshold cryptography based access control scheme is the best in terms of performance (assures the same security level with less processing time). Authors made two definitions: *Verifiability*, a new member must ascertain the validity of the acquired certificate and secret share. *Traceability*, when the new member detects that its certificate and/or secret are not valid, it must be able to trace bogus partial signatures or shares. Overall, authors main goal here was again the authentication of the P2P users, not their authorization.

C. REPUTATION BASED DISTRIBUTED ACCESS CONTROL

Reputation-based systems are used to establish trust among members of on-line communities where parties with no prior information of each other use the feedback from their peers to assess the trustworthiness of the peers in the community.

The protocol proposed by Selcuk *et al.* [60] is a reputation-based distributed trust architecture for P2P networks which helps establishing trust among good peers as well as identifying the malicious peers and preventing the spread of malicious content In the proposed protocol users rate the reliability of the parties they deal with, and share this information with their peers.

In [61], Tran *et al.* describe the access rule as follows: Any client peer who has its overall trust value and overall contribution score equal to or greater than the corresponding thresholds can access to the file. In the proposed Access Control Framework, provides P2P users better access control services whilst preserving the decentralized structure of the P2P platform. The *peers* in a P2P network need the autonomy of controlling accesses to their files. Discretionary Access Control (DAC) model is used in which the control of access rights is left to the discretion of the owner of the file.

The host peer is a standalone system where shared files are objects that need to be protected and client peers are subjects who are considered to possess access rights. Files on host peer are rated depending on their size and content; each

file being assigned two thresholds which capture two access aspects, namely trust and contribution. Whereas, the client peer is responsible to collect recommendations that contain the information needed to evaluate its access values for a particular host.

After each transaction, direct trust and direct contribution of both the client peer and host peers are updated accordingly to the satisfaction level of the transaction. This affects the future evaluation of the access values between these two peers. The more a peer uploads its files to the network, the more likely that peer will be able to download its desired files from the network.

The authentication and access control layer is responsible for authenticating partner peers, calculating access values, granting access to files, and updating local access control policy.

A fairness-based participation is the main goal here. A client who wishes to download a file needs to have both of its access values (trustworthiness and contribution) equal to or greater than the corresponding thresholds of the file. The access values are relative and assessed on a peer to peer basis. They are computed from combinations of four different scores:

- *Direct trust:* represents the host's belief on the client's capacities, honesty and reliability based on the host's direct experiences.
- *Indirect trust:* based on recommendations from other peers, hence it is based on other's observations, it is less reliable when compared to direct trust.
- *Direct contribution:* measures the contribution of the client to the host in terms of information value downloaded and uploaded between them.
- *Indirect contribution:* measures the contribution of the client to the network in terms of information volume the client exchange with other peers.

The proposed scheme for evaluating a transaction, not only helps to differentiate poorly performing peers from good ones, but also ensures that malicious peers are punished and isolated.

D. TRUSTED COMPUTING BASED DISTRIBUTED ACCESS CONTROL

By using trusted computing technologies, a reference monitor in a platform can act as an agent of an object owner to enforce access control policies, which states that an object can only be accessed in a genuine platform with applications in valid states, such as integrity and configuration.

In [62], Sandhu *et al.* propose the Trusted Reference Monitor (TRM), a trusted computing architecture on the application layer, which provides a solution to access control by using trusted computing. In the proposed scheme, fulfillment of security policies are achieved by the integrity and state of the platform along with the software running on the platform. It uses Trusted Embedded Platforms in order to support access control. The proposed architecture enforces an object owner's policy in a client platform by attesting the authenticity of the platform and the integrity of the requesting application.

A TRM is responsible for ensuring that the resources that it protects do not leak into other applications. The proposed scheme enforces access control policies in the application layer by leveraging underlying trusted computing functions. Hardware and operating system security (secure kernel) are the main concerns of this approach. It provides a solution to access control on application layer by using trusted computing. It focuses on operating system and hardware related security on mobile devices. By using proposed trusted computing technologies, a reference monitor in a platform can act as an agent of an object owner to enforce access control policies, which states that an object can only be accessed in a genuine platform with applications in valid states, such as integrity and configuration.

E. IDENTITY BASED DISTRIBUTED ACCESS CONTROL

In [63], Saxena *et al.* proposed an *Identity-based Access Control* scheme for the groups called ''Identity-based Group Admission Control''. In this proposal, the *communication efficiency* was the primary goal. A prospective member and a set of existing group members interact in order to approve the new membership. The number of current members taking part in the admission should at least be equal to the number necessary for the admission threshold, which is less than the total number of group members. A secure membership revocation is also presented in order to provide a fare network service. The proposed scheme is an alternative to the *Threshold Cryptography (Threshold-signature -based)* solutions and much more applicable than those schemes if communication bandwidth and battery power are of prime concerns.

F. CAPABILITY BASED DISTRIBUTED ACCESS CONTROL

In the proposed *Capability-based Access Control* scheme of Kim *et al.* [64], a client should present a valid capability certificate to access a service. A *Capability Certificate* states that an entity which is able to demonstrate knowledge of the corresponding private key has been transferred the rights listed in the certificate by the issuer. *Digital Signatures* are used to protect capability certificates and if these certificates contain access rights then they are called authorization certificates. Different access rights to a service can be granted depending on authenticated authorization certificates. The proposed scheme builds a multi-layered platform based on a Public Key Infrastructure (PKI), which allows peers to communicate securely. It uses Certificate Revocation Lists (CRL) in order to revoke capabilities from the peers.

In P2P networks, secure transaction is of paramount importance due to sheer size and the policy of non-intervention nature of internet. For instance, let us consider E-speak which was first developed at HP Labs in late 1995 [65]. E-Speak is an e-services infrastructure where services advertise, discover, and inter-operate with each other in a dynamic and secure way. The E-Speak security adopts a multi-layered

approach and builds a range of protection mechanisms on top of the PKI. It offers a range of protection mechanisms including authentication, content integrity, visibility control and capability-based access control. The E-Speak security is designed to prevent attacks ranging from traffic analysis to eavesdropping to message tampering to deletion to identity theft. Deployment assumption of E-Speak security is based on the unavailability of central security administration. The security infrastructure assumed to scale up to millions of machines. Though, it is recommended that *message confidentiality* and *message authentication* should not be taken for granted.

In E-Speak, a client should present a valid capability certificate to access a service. The service authenticates the capability certificate by verifying the client's knowledge of the private key corresponding to the given public key. The results of authentication are cached so that the same authentication need not be repeated on every access. Different access rights to a service can be granted depending on authenticated authorization certificates.

G. ACCESS CONTROL LIST BASED DISTRIBUTED ACCESS CONTROL

An Access Control List (ACL) is a list of permissions attached to an object. An ACL specifies the users and/or system processes that are granted access to the object as well as the operations that are allowed on the given objects. Typically, each entry in an ACL specifies a subject and an operation. In [66], Fenkam *et al.* provide a solution to implement access control for mobile P2P systems in collaborative environments. The system provides access control services in mobile teamwork platform (MOTION) in which team members communicate in a P2P manner. Two categories of peers are distinguished, Level-1 (L1) and Level-2 (L2): *L1 peers* have the capacity of maintaining a regular security infrastructure and are superior than L2 peers. They have complete intelligence for assigning permissions, removing permissions, validating and storing ACLs. *L2 peers* have devices which are lacking resources to maintain a regular security infrastructure.

A community leader (L1 peer) can be defined for each community and can be given the right to further assign this right to members (L2 peers) of the community. In a *multi-layered access control approach*, permissions (in the form of ACLs) are distributed according to the capacity of the peers' resources.

H. GROUP SIGNATURE BASED DISTRIBUTED ACCESS CONTROL

A *peer group* is characterized by a flat structure meaning that there is no hierarchy among members and all members have identical rights and duties. There is no underlying assumption of a centralized authority that provides security services such as access control or key management. In group environments where secure any-to-any communication among all members is needed, group admission needs to be tightly integrated with group key management.

In group signature schemes, all group members are peers and any member can sign on behalf of the group in an anonymous and unlinkable manner. Therefore, neither online presence of all signers nor membership awareness is necessary, which is practical for asynchronous groups. In [67], Kim *et al.* proposed group admission is as three steps:

1) Creation of the group charter (ACL).
2) Interaction between a prospective member and the group (voting).
3) Interaction between the new group member and the group authority.

The group authority presents an access control file for different kinds of peer groups and matches them with appropriate cryptographic techniques and protocols.

I. HYBRID DISTRIBUTED ACCESS CONTROL

In order to provide stronger security, *hybrid distributed access control schemes* inherit 2 or more of the access control schemes presented above.

The solution proposed by Lu *et al.* [68] integrates the credential-based, identity-based, and role-based access control policies. A role mapping technique is employed which does not require centralized authority. This paper presents primary copy/backup copy (PB) architecture to support a decentralized access control, not only for usability and scalability, but also for security particularly. The PB strategy is employed to take the function of fault-tolerant network structure and has been used for fault-tolerant dynamic scheduling of tasks in multiprocessor systems.

Another solution proposed by Tseng *et al.* [69] integrates the threshold cryptography-based (Feldman's threshold private key generation), the secret sharing-based (Pederson's distributed secret sharing function generation), and the hierarchical identity-based (Gentry-Silverberg's encryption/signature) access control policies all together. The proposed scheme is called hierarchical identity based PKI (HIDPKI) and supports secure opportunistic collaboration among peers. It operates in server-less environments. Admission of new peer nodes and maintenance of peer administrative domains are managed by groups of peers capable of performing verifiable secret sharing and joint secret sharing operations. HIDPKI provides peer nodes with private keys that match with public keys derived from the identity of the peer nodes and the services they are authorized to offer or use.

IV. APPLICABILITY OF LEGACY P2P ACCESS CONTROL SCHEMES TO BLOCKCHAIN SYSTEMS FOR IoT

As the name implies, centralized P2P access control schemes such as RBAC schemes, require centralized administration of the roles, users and transactions. Therefore, they are not applicable to Blockchain Systems (BCSs) for IoT, in which de-centralization of the control (distributed decision-taking)

TABLE 1. Applicability of Legacy P2P Access Control Schemes to Blockchain Systems for IoT including pros vs. cons.

Access control approach	Decision taking	Related literature	Pros	Cons	Applicability to IoT-based BCSs
RBAC	Centralized	[56], [57]	easy assignment of the access control to the users base on their roles	requires central administration in a centralized network	✖
Threshold-signature	Distributed	[58], [59]	provides central administration in a distributed network, easy inclusion and revocation of the nodes	needs several nodes to be involved on the decision making process	✔
Reputation	Distributed	[60], [61]	reward based scheme, which encourages nodes to be cooperative	requires time for new nodes to be included in the network	✔
Trusted-computing	Distributed	[62]	provides central administration in a distributed network	establishment of trust in a distributed network	✔
Identity	Distributed	[63]	communication bandwidth and battery power	requires identification and against user anonymity	✖
Capability	Distributed	[64] [65]	seamless and easy management	requires digital signatures and PKI	■
ACL	Distributed	[66]	seamless and easy management	requires hierarchical network	✖
Group-signature	Distributed	[67]	consensus-based agreement	requires identical nodes	✔
Hybrid	Distributed	[68], [69]	interoperability	requires identification	✖

Legend: ✔:applicable, ■:applicable but not suggested, ✖:not-applicable.

is the main goal. The details of the different distributed P2P access control schemes are outlined below, also see Table 1 for their applicability to BCSs for IoT, including pros vs. cons of each P2P access control scheme:

- **Threshold-signature -based** requires distributed administration and provides a good solution for authentication and revocation steps of the access control, hence applicable to BCSs for IoT.
- **Reputation-based** system is efficient for user rating and would be partially included in the authorization step. The more a user contributes, the more access rights he/she may get. This is applicable to BCSs for IoT. The more reputed nodes can process more blocks and non-reputed ones process less.
- **Trusted-computing -based** access control scheme requires distributed administration and provides suitable solution for authorization step of the BCSs for IoT.
- **Identity-based** access control solution requires identification of the users, therefore might not be feasible for the BCSs for IoT (in some specific blockchain applications, user anonymity might be most desired feature of the system).
- **Capability-based** access control solution requires digital signatures and therefore PKI architecture. Although this is possible and applicable to BCSs for IoT, it might not be a suggested solution as construction and maintenance of PKI infrastructure would bring extra burden to the overall system performance.
- **ACL-based** access control solution requires hierarchical network structure (L1 and L2 peers). Hence BCSs use identical nodes to process the blocks of the ledgers, ACL-based access control solution cannot be applied.
- **Group signature-based** access control solution allows each member of the group to sign on behalf of the group in an anonymous and unlinkable way. This is very applicable to BCSs, where peers are identical and there is no hierarchy.
- **Hybrid** schemes also use identity-based access control as a part of their solution, hence not applicable to BCSs for IoT.

V. APPLICATION OF PERMISSIONED-BLOCKCHAIN SYSTEMS TO IoT NETWORKS

As mentioned earlier in this text, permissioned-BCSs can be a remedy in securing IoT systems.

Various cyber-security solutions can be provided to several entities of the IoT networks by leveraging permissioned-BCSs, as shown in Figure 3:

1) **Nodes (End-devices [*ED*s]):** Physical capture threat against *ED*s and eventually extraction of security parameters can be neutralized by usage of simple challenge-response protocol in between *ED*s and *GW*, which then can be logged in to the blockchain for future inspections of the events.
2) **Gateway (*GW*s):** An authentication mechanism for the *GW*s is necessary in order to prevent the network from *Rogue-Gateway* attacks. For instance, a mutual authentication can be performed in between the couples of *ED-GW* and *GW-NS*, which then can be logged in to the blockchain for future inspections of the events.
3) **Servers:** In IoT, servers need to be trusted entities, otherwise they can create single point of failure for the network. This should be solidified with some professional advice and/or by providing trust related algorithm suggestions for the server side implementations. This can be achieved by running trust assuring algorithms and which also can be logged in to the blockchain for future inspections of the events.

VI. OPEN ISSUES AND RESEARCH DIRECTIONS

The open issues in application of BCSs towards the security of IoT networks can be categorised as follows [37]:

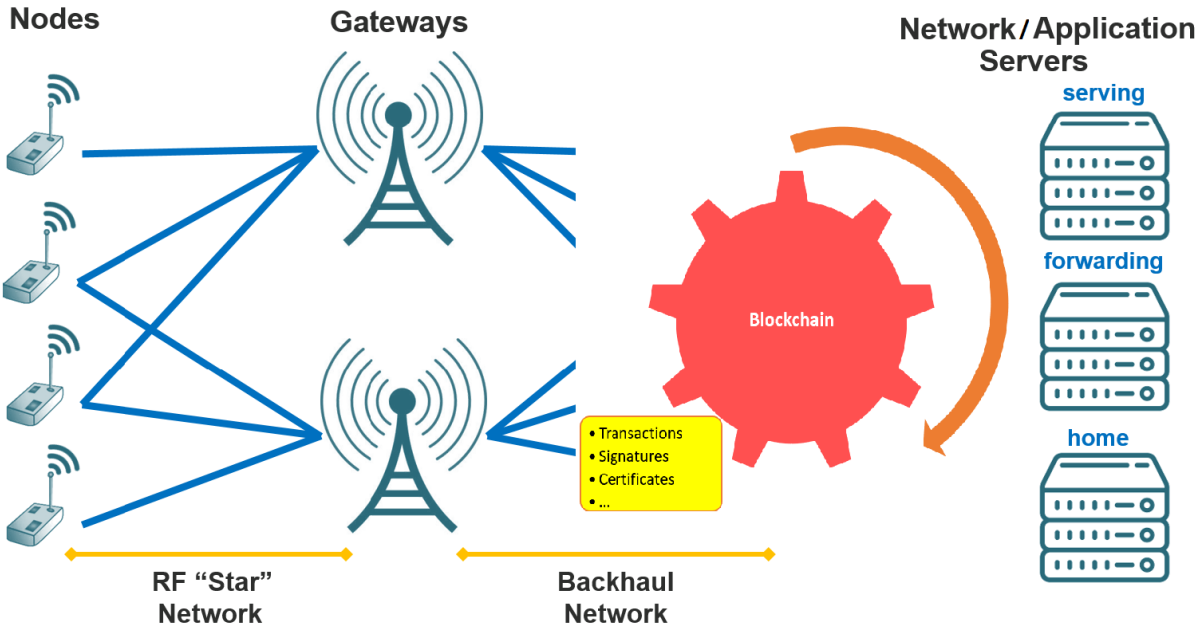

FIGURE 3. A typical IoT network architecture served by Blockchain consensus for various purposes.

1) **Scalability:** Scalability is related to the capacity and constitutes one of the major problems faced by recent blockchain-based IoT applications. In the case of financial and monetary transactions, several thousands of transaction per second happens instantly. However, this cannot be handled with today's IoT infrastructure. The challenge of scalability for blockchain systems emanates from the fact that current consensus mechanisms and blockchain structures are not efficient and suited for IoT. This would eventually result in slow validation of the transactions due to long synchronization time, high transaction costs due to large memory storage and processing power requirements.
2) **Interoperability:** As mentioned earlier, either designed for IoT or not, various BCSs are devised to remedy special problems of different applications along with specific constraints and requirements. Thereby, there is no unique BCS skeleton that can be adopted by each and every other application. Recently, the ecosystem of the blockchain is very scattered around as BCSs have their own protocols, functions and mechanisms that are not inter operable with each other. It is obvious that there will be necessarily many BCSs exist and they have to be designed in accordance to each other so that they can operate and interact with each other in a seamless way.
3) **Lightweight Consensus Algorithms:** As stated earlier, BCSs are power, processor and memory hungry and do not directly suited for IoT networks. Therefore, in order to apply BCSs to IoT and for the long term acceptance of the BCSs by the IoT community; 'lightweight' consensus algorithms are required by addressing the various problems (resource [power, memory, processing, etc.] consumption, limited throughput, delay, etc.).

Under the light of the challenges and open problems presented above, the research directions in application of BCSs towards the security of IoT networks can be summarized as follows:

- **Cyber-Security Analysis:** A better understanding of the system behavior from the cyber-security perspective can be orchestrated via vulnerability and attack analysis. The system consistency of the blockchain-based IoT system can be monitored and verified to detect any potential changes from the nominal behavior.
- **Performance Analysis:** The end-to-end performance analysis of the BCS can be investigated for a complete cycle of the blockchain, from submitting till when the related block is engraved in to the blockchain.
- **Feasibility Analysis:** There are 3 types of feasibility analysis: *1) Technical feasibility:* Integration of existing systems with the BCSs introduces a big technical complexity and more costs towards the design, development, and maintenance phases. *2) Operational feasibility:* The operation mode of BCSs differ from traditional cloud-based systems as BCSs have previously mentioned drawbacks and challenges as much as the advantages they bring. For instance, commercially sensitive information should not be stored at public BCSs as protection of the the secret is naively impossible there. Moreover, owing to the immutability of BCSs, it requires extra attention and effort for renewing smart contracts on the blockchain. *3) Economic feasibility:*

An intended vendor need to analyze the cost of storing the generated data on the public or private blockchain along with the cost of executing and deploying the smart contracts or certificates. In order to have an understanding on the feasibility of the BCSs to IoT networks, all 3 of the mentioned feasibility analyses should be run.

- **Cost Analysis:** This is another important ingredient that needs to be taken into account in the overall assessment. The cost analysis is dependent to many other sub-components: 1) *Monetary cost:* It is about storing the data and executing a smart-contract on the BCS. 2) *Keeping cost:* This is the cost to keep the blockchain nodes employed by the BCS application. Even though this is not a requirement, having your own blockchain nodes to calculate block operations might significantly enhance the system response time and decrease overall latency. Moreover, if Proof-of-Work is used as the consensus algorithm, then the cost of keeping your own blockchain infrastructure might be really costly.

VII. CONCLUSION AND FUTURE WORK

As in any computer system, access control is a very important function of securing Blockchain Systems (BCSs). The overall procedure for access control in BCSs will require three main steps, namely: authentication, authorization, and revocation. Performance, cost, and scalability are the main challenges when integrating blockchain with IoT, owing to the high volume of data generated by IoT networks. Therefore, permissioned BCSs would be more suitable than permissionless BCSs for IoT platforms. Consequently, this article described how permissioned BCSs can be leveraged by IoT networks to increase the security of the network.

Providing access control functionality for permissioned BCSs is a non-trivial task. In this article, a remedy to this is provided by investigating the state of the art access control schemes proposed for P2P networks and elaborating on their applicability to permissioned BCSs. Table 1 presents all investigated access control schemes along with their applicability to permissioned BCSs.

From the thorough literature review on P2P systems, it is deduced that a reasonable access control system proposal for the permissioned BCSs should include the following approaches: A threshold signature-based system for the authentication step, a trusted computing-based system along with a reputation-based system for the authorization step, and finally, CRL along with a group signature-based system for the revocation step. The mentioned steps increase the security and overall trust of the system. However, applicability to IoT networks, such as the LoRa-based networks discussed in this text, needs further investigation and attention, especially in terms of power consumption and packet delay.

In this article, contrary to some other proposals in the literature and due to their long processing times for each transaction (consensus), the authors aim is to avoid the usage of BCS directly for access control, instead of providing distributed P2P access control methods as an access control mechanism for permissioned BCSs. After users are granted for permissioned BCSs, these can be leveraged by the users for some other purposes such as data logging, archiving, etc.

Establishing control over cross interactions of the access control schemes and evaluating their effect on the overall efficiency of the access control system is a non-trivial task. The system design and implementation of the presented access control schemes for permissioned BCSs are therefore left as future work.

APPENDIX
ABBREVIATIONS AND ACRONYMS

List of abbreviations are listed in Table 2.

TABLE 2. List of abbreviations.

Abbreviation	Explanation
ACL	Access Control List
ADL	Activity of daily living
AS	Application Server
ASM	Accountable Subgroup Multi-signature
BCS	Blockchain System
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DoS	Denial-of-Service
DSA	Digital Signature Algorithm
ED	End Device
EUI	Extended Unique Identifier
GDPR	European General Data Protection Regulation
GMC	Group Membership Certificates
GW	GateWay
HIDPKI	Hierarchical IDentity-based PKI
IoT	Internet of Things
ITS	Intelligent Transportation System
LoRa	Long Range communications for IoT
LoRaWAN	LoRa-based Wide Area Network
MITM	Man-In-The-Middle
NS	Network Server
PB	Primary/Backup copy
PKI	Public Key Infrastructure
PS	Plain signature
P2P	Peer-to-Peer
PUF	Physical Unclonable Function
RBAC	Role-based Access Control
RSA	Rivest-Shamir-Adleman
SDN	Software Defined Network
TRM	Trusted Reference Monitor
TTP	Trusted Third Party
VoIP	Voice over Internet Protocol

REFERENCES

[1] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards Internet of Things," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–6.

[2] *Internet of Things at a Glance*. Accessed: Dec. 10, 2019. [Online]. Available: https://cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/cisco.com

[3] I. Butun, N. Pereira, and M. Gidlund, "Analysis of lorawan v1.1 security: Research paper," in *Proc. 4th ACM MobiHoc Workshop Exper. With Design Implement. Smart Objects (SMARTOBJECTS)*, New York, NY, USA, 2018, pp. 5:1–5:6.

[4] I. Butun, N. Pereira, and M. Gidlund, "Security risk analysis of LoRaWAN and future directions," *Future Internet*, vol. 11, no. 1, p. 3, Dec. 2018.

[5] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of LoRaWAN," *Comput. Netw.*, vol. 148, pp. 328–339, Jan. 2019.
[6] J. de Carvalho Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic, and A. L. L. Aquino, "LoRaWAN—A low power wan protocol for Internet of Things: A review and opportunities," in *Proc. 2nd Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech)*, 2017, pp. 1–6.
[7] J. Wu, Y. Feng, and P. Sun, "Sensor fusion for recognition of activities of daily living," *Sensors*, vol. 18, no. 11, p. 4029, Nov. 2018.
[8] D. Puri. *IoT and LoRaWAN Modernize Livestock Monitoring*. Accessed: Feb. 10, 2020. [Online]. Available: http://www.braemacca.com/en/news/item/iot-and-lorawan-modernize-livestock-monitoring
[9] I. Butun and R. Sankar, "A brief survey of access control in wireless sensor networks," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2011, pp. 1118–1119.
[10] V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, and S. Kanhere, "Blockchain technologies for IoT," in *Advanced Applications of Blockchain Technology*. Singapore: Springer, 2020, pp. 55–89.
[11] S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access*, vol. 7, pp. 58822–58835, 2019.
[12] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.
[13] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in *Sequences II*. New York, NY, USA: Springer, 1993, pp. 329–334.
[14] F. A. von Hayek, *Denationalisation of Money: An Analysis of the Theory and Practice of Current Currencies*. London, U.K.: Institute of Economic Affairs, 1976.
[15] J. E. McDonald, "The tokenization of industrial cryptocurrency mining," Ormeus Coin, White Paper, 2018, pp. 1–21.
[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
[17] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar Publishing, 2016.
[18] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.
[19] M. Dabbagh, M. Sookhak, and N. S. Safa, "The evolution of blockchain: A bibliometric study," *IEEE Access*, vol. 7, pp. 19212–19221, 2019.
[20] S. Dewan and L. Singh, "Use of blockchain in designing smart city," *Smart Sustain. Built Environ.*, vol. 9, no. 4, pp. 695–709, Mar. 2020.
[21] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.
[22] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.
[23] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.
[24] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.
[25] T. A. Ahanger and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019.
[26] I. Butun, A. Sari, and P. Osterberg, "Security implications of fog computing on the Internet of Things," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–6.
[27] A. Sari, A. Lekidis, and I. Butun, "Industrial networks and IIoT: Now and future trends," in *Industrial IoT*. Cham, Switzerland: Springer, 2020, pp. 3–55.
[28] I. Butun, A. Sari, and P. Österberg, "Hardware security of fog end-devices for the Internet of Things," *Sensors*, vol. 20, no. 20, p. 5729, Oct. 2020.
[29] *Peer-to-Peer*. Accessed: Sep. 23, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Peer-to-peer
[30] H. M. N. D. Bandara and A. P. Jayasumana, "Collaborative applications over peer-to-peer systems–challenges and solutions," *Peer-Peer Netw. Appl.*, vol. 6, no. 3, pp. 257–276, Sep. 2013.
[31] *Dalesa*. Accessed: Sep. 23, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Dalesa
[32] *Voice Over IP (VoIP)*. Accessed: Sep. 23, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Voice_over_IP
[33] H. S. Kenyon. *Multispectral Camera System to Provide Soldiers With Enhanced Night Vision*. Accessed: Sep. 23, 2020. [Online]. Available: https://www.afcea.org/content/multispectral-camera%E2%80%A8-system-provide-soldiers%E2%80%A8-enhanced-night-vision
[34] I. Butun, "Prevention and detection of intrusions in wireless sensor networks," Ph.D. dissertation, Univ. South Florida, Tampa, FL, USA, 2013.
[35] M. Vukolić, "Rethinking permissioned blockchains," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, Apr. 2017, pp. 3–7.
[36] T. Swanson, "Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems," Post Oak Labs, USA, Tech. Rep., Apr. 2015.
[37] S. Kim and G. C. Deka, *Advanced Applications of Blockchain Technology*. Singapore: Springer, 2020.
[38] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara, "Capability-based access control for the Internet of Things: An ethereum blockchain-based scheme," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[39] D. Chattaraj, S. Saha, B. Bera, and A. K. Das, "On the design of blockchain-based access control scheme for software defined networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 237–242.
[40] I. Riabi, H. K. B. Ayed, and L. A. Saidane, "A survey on blockchain based access control for Internet of Things," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 502–507.
[41] I. Riabi, Y. Dhif, H. K. B. Ayed, and K. Zaatouri, "A blockchain based access control for IoT," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 2086–2091.
[42] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou, "Blockchain-based consents management for personal data processing in the IoT ecosystem," in *Proc. 15th Int. Joint Conf. e-Bus. Telecommun.*, 2018, pp. 738–743.
[43] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the Internet of everything (IoE)," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 8–16, Mar. 2020.
[44] J. Lin, W. Long, A. Zhang, and Y. Chai, "Using blockchain and IoT technologies to enhance intellectual property protection," in *Proc. 4th Int. Conf. Crowd Sci. Eng.*, Oct. 2019, pp. 44–49.
[45] M. Wazid, A. K. Das, S. Shetty, and M. Jo, "A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things," *IEEE Access*, vol. 8, pp. 88700–88716, 2020.
[46] M. Wazid, A. K. Das, S. Shetty, and J. J. P. C. Rodrigues, "On the design of secure communication framework for blockchain-based Internet of intelligent battlefield things environment," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 888–893.
[47] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, Jul. 2020.
[48] F. Kandah, B. Huber, A. Altarawneh, S. Medury, and A. Skjellum, "BLAST: Blockchain-based trust management in smart cities and connected vehicles setup," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2019, pp. 1–7.
[49] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
[50] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo, "Blockchain-enabled cyber-physical systems: A review," *IEEE Internet Things J.*, early access, Aug. 6, 2020, doi: 10.1109/JIOT.2020.3014864.
[51] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. H. Park, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors J.*, early access, Jul. 15, 2020, doi: 10.1109/JSEN.2020.3009382.
[52] M. D. Borah, V. B. Naik, R. Patgiri, A. Bhargav, B. Phukan, and S. G. Basani, "Supply chain management in agriculture using blockchain and IoT," in *Advanced Applications of Blockchain Technology*. Singapore: Springer, 2020, pp. 227–242.
[53] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, "A lightweight blockchain based framework for underwater IoT," *Electronics*, vol. 8, no. 12, p. 1552, Dec. 2019.

[54] S. Makridakis and K. Christodoulou, "Blockchain: Current challenges and future prospects/applications," *Future Internet*, vol. 11, no. 12, p. 258, Dec. 2019.
[55] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Trans. Inf. Syst. Secur.*, vol. 4, no. 3, pp. 224–274, Aug. 2001.
[56] J. S. Park, G. An, and D. Chandra, "Trusted P2P computing environments with role-based access control," *IET Inf. Security*, vol. 1, no. 1, pp. 27–35, Mar. 2007.
[57] J. S. Park and J. Hwang, "Role-based access control for collaborative enterprise in peer-to-peer computing environments," in *Proc. 8th ACM Symp. Access Control Models Technol. (SACMAT)*, 2003, pp. 93–99.
[58] N. Saxena, G. Tsudik, and J. H. Yi, "Admission control in peer-to-peer: Design and performance evaluation," in *Proc. 1st ACM Workshop Secur. Ad Hoc Sensor Netw. (SASN)*, 2003, pp. 104–113.
[59] N. Saxena, G. Tsudik, and J. Hyun Yi, "Access control in ad hoc groups," in *Proc. Int. Workshop Hot Topics Peer-Peer Syst.*, 2004, pp. 2–7.
[60] A. A. Selcuk, E. Uzun, and M. R. Pariente, "A reputation-based trust management system for P2P networks," in *Proc. IEEE Int. Symp. Cluster Comput. Grid (CCGrid)*, Apr. 2004, pp. 251–258.
[61] H. Tran, M. Hitchens, V. Varadharajan, and P. Watters, "A trust based access control framework for P2P file-sharing systems," in *Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2005, p. 302.
[62] R. Sandhu and X. Zhang, "Peer-to-peer access control architecture using trusted computing technology," in *Proc. 10th ACM Symp. Access Control Models Technol. (SACMAT)*, 2005, pp. 147–158.
[63] N. Saxena, G. Tsudik, and J. H. Yi, "Identity-based access control for ad hoc groups," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Berlin, Germany: Springer, 2004, pp. 362–379.
[64] W. Kim, S. Graupner, and A. Sahai, "A secure platform for peer-to-peer computing in the Internet," in *Proc. 35th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2002, pp. 3948–3957.
[65] A. H. Karp, "E-speak e-xplained," *Commun. ACM*, vol. 46, no. 7, pp. 112–118, Jul. 2003.
[66] P. Fenkam, S. Dustdar, E. Kirda, G. Reif, and H. Gall, "Towards an access control system for mobile peer-to-peer collaborative environments," in *Proc. 11th IEEE Int. Workshops Enabling Technol., Infrastruct. Collaborative Enterprises (WET ICE)*, 2002, pp. 95–100.
[67] Y. Kim, D. Mazzocchi, and G. Tsudik, "Admission control in peer groups," in *Proc. 2nd IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, 2003, pp. 131–139.
[68] J. Lu, R. Li, Z. Lu, and X. Ma, "A role-based access control architecture for P2P file-sharing systems using primary/backup strategy," in *Proc. Int. Conf. Netw. Secur., Wireless Commun. Trusted Comput. (NSWCTC)*, vol. 1, Apr. 2009, pp. 700–703.
[69] F.-K. Tseng, J. K. Zao, Y.-H. Liu, and F.-P. Kuo, "Halo: A hierarchical identity-based public key infrastructure for peer-to-peer opportunistic collaboration," in *Proc. 10th Int. Conf. Mobile Data Manage., Syst., Services Middleware (MDM)*, 2009, pp. 672–679.

ISMAIL BUTUN (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical and electronics engineering from Hacettepe University, in 2003 and 2006, respectively, and the M.Sc. degree and the Ph.D. degree in electrical engineering from the University of South Florida, in 2009 and 2013, respectively. From 2014 to 2015, he worked as an Assistant Professor with the Department of Mechatronics Engineering, Bursa Technical University. He has worked as a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Delaware, in 2016. He was affiliated as an Assistant Professor with the Department of Computer Engineering, Abdullah Gul University, in 2017. Since 2019, he has been working as a Postdoctoral Fellow with the Department of Computer Science and Engineering, Chalmers University of Technology. His research interests include computer networks, wireless communications, the Internet of Things, cryptography, network security, and intrusion detection.

PATRIK ÖSTERBERG (Member, IEEE) received the M.Sc. degree in electrical engineering from Mid Sweden University, Sundsvall, Sweden, in 2000, the degree of Licentiate of Technology in teleinformatics from the Royal Institute of Technology, Stockholm, Sweden, in 2005, and the Ph.D. degree in computer and system science from Mid Sweden University, in 2008. He worked as a Development Engineer with Acreo AB, Hudiksvall, Sweden, in 2007. From 2008 to 2010, he was employed as a Researcher with Interactive TV Arena KB in Gävle, Sweden. Since 2008, he has been an Assistant Professor with Mid Sweden University, where he was appointed as the Head of the Department of Information and Communication Systems, from 2013 to 2017. Since 2018, he has been the Head of the Department of Information Systems and Technology, Mid Sweden University.